Deterministic unitary operations on time-bin qudits for quantum communication

Félix Bussières,* Yasaman Soudagar, Guido Berlin, Suzanne Lacroix, and Nicolas Godbout

Centre d'optique, photonique et lasers, Laboratoire des fibres optiques,
Département de génie physique, École Polytechnique de Montréal,
C.P. 6079, Succ. Centre-ville, Montréal (QC), H3C 3A7 Canada
(Dated: February 1, 2008)

We show for the first time how deterministic unitary operations on time-bin qubits encoded in single photon pulses can be realized using fiber optics components that are available with current technology. We also generalize this result to operations on time-bin qudits, i.e. d-level systems, and show that this can be done efficiently using 2×2 beamsplitters and phase modulators. Important benefits for experimental quantum communication are highlighted. This work shows how to bridge the gap between current proof-of-principle demonstrations and complete, deterministic experiments.

Quantum information science is rooted in the idea that information can be encoded and processed in qubits, i.e. two-level quantum systems [1]. Recently, this fruitful proposition led to important theoretical results in the field of quantum communication along with experimental demonstrations of quantum cryptography [2], quantum repeaters [3], tests of Bell's theorem [4] and quantum teleportation [5] (see Ref. 6 for a review). Moreover, there are now numerous proposals benefiting from the use of qudits (d-level quantum systems). In cryptography, qudits increase the tolerance to noise [7] and in quantum communication, they improve channel capacity [8]. When entangled, they enhance the security bounds for coin flipping [9], they reduce the communication complexity below the classical limit [10] and they give a solution to the Byzantine agreement problem [11]. Entangled qudits are also useful for testing Bell's theorem by providing a stronger violation [12] and a greater robustness against noise [13].

Photons and optical fiber are natural candidates to implement quantum communication protocols and for this purpose, the time-bin encoding for qubits is proven to be very robust and practical [14, 15]. To generate a time-bin qubit, a single photon pulse is first split in two rails using a 2×2 coupler (the all-fiber equivalent of a beamsplitter) as shown on Fig. 1. Then, each component travels through either the "short" or "long" rails. Finally, both are time-multiplexed in the same fiber using a 2×1 optical switch. At the output, the single photon is in a coherent superposition of being in two time-bins separated by a delay Δt: $|\psi\rangle = \alpha|\text{short}\rangle + \beta|\text{long}\rangle$. By changing the coupling ratio of the coupler and the phase delay φ of the phase modulator, all pure qubit states can be generated. Time-bin entanglement in the state $\alpha|\text{short, short}\rangle + \beta|\text{long, long}\rangle$ can also be generated efficiently using spontaneous parametric downconversion [15]. This type of entanglement has been shown to be robust against polarization mode dispersion, phase fluctuations and chromatic dispersion over at least 50 km of transmission in optical fiber [16, 17].
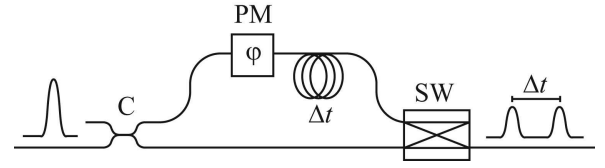

FIG. 1: Experimental set-up to generate time-bin qubits. Lines are optical fibers, C is a coupler (the all-fiber equivalent of a beamsplitter), PM is a phase modulator and SW is a 2×1 optical switch.

The main difficulty with time-bin encoding is that both single qubit unitary operations and measurements in any basis are not trivial to implement. Actually, most of the experiments done so far use non-deterministic operations with post-selection [6, 18, 19] and this reduces the success rate, if not leading to a complete failure. For example, complete quantum teleportation of a time-bin qubit cannot be achieved without using deterministic single qubit operations to correct the teleported state [19]. A similar problem exists in the experiments testing Bell's theorem with time-bin qubits as we discuss below. Also, multi-user protocols requiring cascaded operations on the same qubit are not scalable when limited to probabilistic operations. The ubiquitous need for single time-bin qubit and qudit deterministic operations for quantum communication and the lack of any general scheme to do this are the motivations of this work. In this letter, we extend on our work of Ref. 20 and propose different experimental schemes to perform deterministic unitary operations on time-bin qubits and qudits using photons. These schemes can be implemented with technology that is currently available. Throughout the text, the schemes are presented with single mode optical fiber circuits and wavelengths around 1550 nm. Nevertheless, they can be directly adapted to any kind of waveguide or free-space transmission.

All unitary operations on a single polarization qubit are easy to implement using an all-fiber polarization controller. The first scheme we propose takes advantage of

this by converting a time-bin qubit to a polarization qubit to perform the operation and then converting back to a time-bin qubit for transmission. The gate is shown
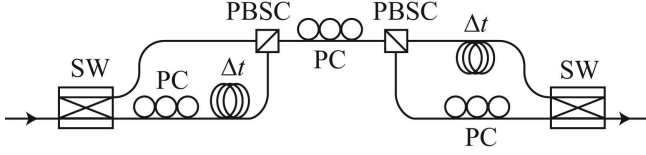

FIG. 2: Experimental layout of the time-bin gate using polarization. Lines are optical fibers, SW is a 1×2 optical switch, PC is a polarization controller and PBSC is a polarization beam splitter/combiner.

on Fig. 2. First, a single photon in a time-bin qubit state with a given polarization, say horizontal (H), is incident from the left on the 1×2 switch which routes the $|short\rangle$ and the $|long\rangle$ components to the lower and upper rails respectively. The polarization of the lower rail is flipped to vertical (V) by a polarization controller and is also delayed by Δt. This delay synchronizes the $|short\rangle$ and $|long\rangle$ components at the inputs of the polarizing beam splitter/combiner (PBSC). The latter reflects and transmits V and H polarizations, hence, the time-bin qubit is converted to a single-rail polarization qubit according to the mapping $|short\rangle \rightarrow |V\rangle$ and $|long\rangle \rightarrow |H\rangle$. Then, the output of the PBSC is fed into an all-fiber polarization controller that transforms any polarization to any other with negligible loss. After the rotation, the polarization qubit is converted back to an H polarized time-bin qubit using the inverse of the operation done in the first section. Therefore, this gate can implement all unitary operations on a single time-bin qubit.

To implement a given operation, the switches are the only active components. The faster the switching speed, the smaller is the required separation between the $|short\rangle$ and $|long\rangle$ components, thus, the smaller is the required path length difference. With current technology, electrooptic material allow for switching frequencies of at least 10 GHz, hence, the path length difference can be set at about 2 cm in standard single mode fiber. This is crucial since the relative phase between the branches has to be stabilized in temperature. A path difference of 2 cm would require the temperature to be stable within 1 tenth of a degree Kelvin at room temperature, which is not difficult to achieve in the laboratory. The two PBSC can be fabricated with fused fiber couplers and are therefore practically lossless [21]. The major limiting factor is the insertion loss of the switches caused mainly by the mode mismatch between the fiber core and the waveguide of the switch. With current technology, this loss can be lowered down to about 1.5 dB for a total of 3 dB for the whole gate.

The second scheme for deterministic operations we propose works by converting the time-bin qubit to a dual-rail qubit for processing [22]. The gate is pictured in Fig. 3 and works as follows. A time-bin qubit is incident from the left on a 1×2 optical switch that routes the $|short\rangle$ and the $|long\rangle$ components to the upper and lower rails respectively. Next, the upper rail is delayed by Δt to syn-
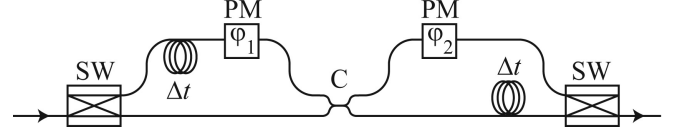

FIG. 3: Experimental layout of the time-bin gate using dual-rail encoding. Lines are optical fibers, SW is a 1×2 optical switch, PM are phase modulators and C is a coupler.

chronize $|short\rangle$ with $|long\rangle$ and consequently, the photon is converted to the dual-rail encoding: $|short\rangle \rightarrow |1\rangle_u|0\rangle_l$ and $|long\rangle \rightarrow |0\rangle_u|1\rangle_l$, where the labels u and l stand for the upper and lower rails respectively. The two components of the single photon interfere at the coupler set to a specific coupling ratio to implement a given gate. This, supplemented with two phase modulators, can implement any unitary operation on the dual-rail qubit. The remaining part of the gate converts the dual-rail qubit back to a single-rail time-bin qubit. Therefore, this gate can implement all unitary operations on a single time-bin qubit.

To implement a given operation, the switches are the only active components and the temperature requirements are the same as in the previous scheme. Moveover, stable and precise phase modulators can be made lossless using piezoactuators glued on the fiber. Finally, the typical loss of an all-fiber coupler is of the order of 0.1 dB or less. Therefore, the only important sources of loss are the switches and again, it can be lowered down to about 3 dB in total. The main advantage of this scheme over the previous one is that it can be made insensitive to alignment if polarization independent switches are used. Also, this scheme is well suited for tasks that require ultra-fast and deterministic feedforward processing like quantum teleportation. Indeed, an ultra-fast tunable coupler can be made with a Mach-Zehnder interferometer using an eletrooptic phase modulator in one of its arms, hence yielding a single circuit that can implement all operations. Using theses ideas, we have shown how the cluster state model of quantum computation can be implemented in optical fiber circuits [23].

We now discuss how this scheme is useful for testing Bell's theorem [4] with time-bin qubits. The robustness of time-bin entanglement over fiber transmission is clearly an advantage to eliminate the locality loophole. However, the detection loophole cannot be closed without using deterministic measurements in the time-bin basis. Indeed, this is essential to overcome the 83% detection efficiency threshold needed to achieve a loophole free violation of the CHSH inequality [24]. To eliminate the de-

tection loophole using the schemes proposed here, one uses the dual-rail gate of Fig. 3 modified such that two detectors are placed on the rails right after the coupler, as shown on Fig. 4. To deterministically measure in any desired basis, one can set the correct values for the coupling ratio and the phase φ_1. Hence, in principle, a simultaneous closure of the detection and locality loopholes is possible using this setup. Encouragingly, we note that a noiseless photon detector with 88% detection efficiency at 1550 nm is now available [25]. With the improvements on optical components, it is reasonable to hope that a loophole free experiment using time-bin qubits and deterministic measurements will be performed in the near future.
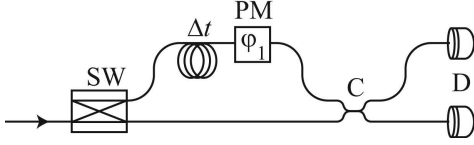

FIG. 4: Experimental layout of the time-bin gate to measure in any desired basis. Lines are optical fibers, SW is a 1×2 optical switch, PM is a phase modulator, C is a coupler and D is a detector.

Before generalizing to deterministic operations on d-level systems, we mention that time-bin qudits can be generated with a setup similar to the one described in Fig. 1, where the single photon is split into d rails instead of two, all of which are time-multiplexed in one fiber using a d×1 switch. Moreover, entangled time-bin qudits have been successfully generated using a mode-locked laser [26].

The generalization to qudit operations is based on the following results: 1 - Time-bin qudits can be easily converted to rail qudits by demultiplexing the bins in d rails using a 1×d switch and by synchronizing all the components with delay lines, 2 - Arbitrary unitary operations on rail qudits can be implemented using 2×2 couplers only [27]. We describe the second result in detail. Consider a single photon in a superposition of being in d rails labelled 1 to d. Let $B_{m,n}$ be the transfer matrix of a lossless 2×2 coupler mixing rails m and n and let $B'_{m,n}$ be the mathematical extension of $B_{m,n}$ to a d×d unitary matrix acting only on the subspace of rails m and n. More precisely, $B'_{m,n}$ consists of the d×d identity matrix I with elements I_{mm}, I_{mn}, I_{nm} and I_{nn} replaced by the elements of $B_{m,n}$. In Ref. 27, it is shown that any d-dimensional unitary transfer matrix U(d) can be factorized in a sequence of $B'_{m,n}$ matrices. The decomposition is written as

$$\mathrm{U}(d) = P \cdot \tilde{B}'_{2,1} \ldots \tilde{B}'_{d-1,1} \cdot \tilde{B}'_{d,1} \,, \tag{1}$$

where $\tilde{B}'_{d,1}$ is a sequence of $d-1$ coupler matices sequentially mixing rails d and $d-1$, d and $d-2$, and so on

until d and 1:

$$\tilde{B}'_{d,1} = B'_{d,1} \ldots B'_{d,d-2} \cdot B'_{d,d-1} \,. \tag{2}$$

The decomposition is similar for $\tilde{B}'_{d-1,1}$, ..., $\tilde{B}'_{2,1}$. The matrix P is a phase correction applied to each mode and requires d phase modulators. Hence, a maximum of $(d-1)(d-2)/2 \sim \mathcal{O}(d^2)$ couplers are necessary to implement any U(d) in the d-rail encoding. As time-bin qudits can always be converted to rail qudits and vice versa, any U(d) can be implemented in the time-bin encoding.

To exemplify our proposition, we illustrate how it can be used to implement the deterministic measurements of the quantum key distribution protocol using qutrits proposed in Ref. 28. This protocol was shown to be more robust to noise than the BB84 protocol using qubits [7]. To generate a key bit, Alice chooses randomly one qutrit state among twelve that are part of four mutually unbiased basis and sends it to Bob. Let $\{|a\rangle, |b\rangle, |c\rangle\}$ be the first orthogonal basis. The second basis can be taken as

$$|a'\rangle = (|a\rangle + |b\rangle + |c\rangle)/\sqrt{3} \,, \tag{3}$$
$$|b'\rangle = (|a\rangle + \mathrm{e}^{2\pi i/3}|b\rangle + \mathrm{e}^{-2\pi i/3}|c\rangle)/\sqrt{3} \,, \tag{4}$$
$$|c'\rangle = (|a\rangle + \mathrm{e}^{-2\pi i/3}|b\rangle + \mathrm{e}^{2\pi i/3}|c\rangle)/\sqrt{3} \,. \tag{5}$$

The third and fourth basis are given by the cyclic permutations of the following states, respectively:

$$(\mathrm{e}^{2\pi i/3}|a\rangle + |b\rangle + |c\rangle)/\sqrt{3} \,, \tag{6}$$
$$(\mathrm{e}^{-2\pi i/3}|a\rangle + |b\rangle + |c\rangle)/\sqrt{3} \,. \tag{7}$$

Upon reception, Bob measures the qutrit in one of the four randomly chosen basis. If the bases match, Alice and Bob keep the results. With time-bin qutrits, Bob can take the first basis to be the time of arrival of the photons. In this case, measurements require only one photon detector and a time frame shared with Alice. However, to measure in the second basis, Bob needs an interferometric setup to apply the unitary transformation $U|\alpha'\rangle = |\alpha\rangle$ in the time-bin encoding, where $\alpha \in \{a, b, c\}$, before measuring with his detector. The matrix U is given by

$$U = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \mathrm{e}^{-2\pi i/3} & \mathrm{e}^{2\pi i/3} \\ 1 & \mathrm{e}^{2\pi i/3} & \mathrm{e}^{-2\pi i/3} \end{pmatrix} \,. \tag{8}$$

Using equation (1), U is factorized as

$$U = P \cdot B'_{2,1} \cdot B'_{3,1} \cdot B'_{3,2} \,, \tag{9}$$

where the 2×2 matrices associated with $B'_{3,2}$, $B'_{3,1}$ and $B'_{2,1}$ are

$$B_{3,2} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathrm{e}^{i\pi/3} & 1 \\ \mathrm{e}^{4\pi i/3} & 1 \end{pmatrix} \,, \tag{10}$$

$$B_{3,1} = \frac{1}{\sqrt{3}} \begin{pmatrix} \sqrt{2}\,\mathrm{e}^{-i\pi/3} & 1 \\ \mathrm{e}^{-i\pi/3} & -\sqrt{2} \end{pmatrix} \,, \tag{11}$$

$$B_{2,1} = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix} \,. \tag{12}$$

The fiber optic circuit implementing U is shown in Fig. 5. First, a 1×3 switch along with delays of Δt and $2\Delta t$ are used to convert the incoming time-bin qutrit to a rail qutrit on which the transformation U is applied using three couplers shown in dashed boxes. In the final section, the resulting qutrit is converted back to the time-bin encoding using a 3×1 switch. The phase correction P is not necessary in this case since detection occurs right after the gate. To measure in the third and fourth basis, it is easy to show that Bob can use the same setup supplemented with phase modulators inserted on all rails between the couplers.
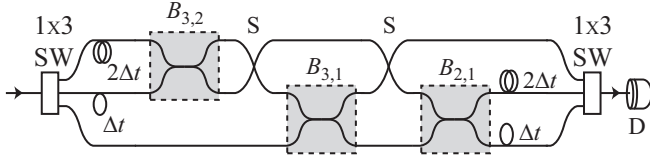

FIG. 5: Experimental layout of the time-bin gate for QKD with qutrits. Lines are optical fibers, SW is a 1×3 optical switch, the dashed boxes show the couplers implementing the unitary transformation on the rail qutrit and S is a rail swap to enable modes 1 and 3 (lower and upper rails) to interfere.

In this letter, we have shown how deterministic unitary operations on single time-bin qubits encoded in photons can be implemented with current optical fiber technology. This also allows to implement deterministic measurements in any basis. Finally the generalization to deterministic operations on time-bin qudits was presented. Ultimately, the schemes are technologically limited by the loss of the switches. Since no physical reason limits the improvements of current optical switches, it is reasonable to believe that experimental quantum communication with time-bin qudits using the schemes presented here will become highly practical in the near future. Future work will focus on the experimental realization of the proposed schemes and on the application to deterministic quantum communication experiments.

* Also at Laboratoire d'informatique théorique et quantique, Université de Montréal, C.P. 6128, Succ. Centre-Ville, Montréal (QC), H3C 3J7 Canada; Electronic address: felix.bussieres@polymtl.ca

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge, 2000).

[2] C. H. Bennett and G. Brassard, in *Proc. of the IEEE Int. conf. on Computers, Systems & Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.

[3] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[4] J. S. Bell, Physics **1**, 195 (1964).

[5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[6] W. Tittel and G. Weihs, Quantum Inf. and Comp. **1**, 3 (2001).

[7] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[8] M. Fujiwara, M. Takeoka, J. Mizuno, and M. Sasaki, Phys. Rev. Lett. **90**, 167906 (2003).

[9] A. Ambainis, in *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC'01)* (ACM Press, New York, 2001), pp. 134–142.

[10] Časlav Brukner, M. Żukowski, and A. Zeilinger, Phys. Rev. Lett. **89**, 197901 (2002).

[11] M. Fitzi, N. Gisin, and U. Maurer, Phys. Rev. Lett. **87**, 217901 (2001).

[12] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).

[13] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).

[14] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[15] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).

[16] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Phys. Rev. Lett. **93**, 180502 (2004).

[17] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, Eur. Phys. J. D **30**, 143 (2004).

[18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. of Mod. Phys. **74**, 145 (2002).

[19] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Nature **421**, 509 (2003).

[20] F. Bussières, Y. Soudagar, G. Berlin, S. Lacroix, and N. Godbout, in *Proc. of IEEE (to be published)* (2006).

[21] M. Aubé, A. Boucon, B. Burgoyne, X. Daxhelet, A. Dupuis, N. Godbout, F. Gonthier, S. Lacroix, M.-E. Leclerc, F. Seguin, et al., Photons: The Technical Review of the Canadian Institute for Photonics Innovations, Spring 2005 (2005).

[22] I. L. Chuang and Y. Yamamoto, Phys. Rev. A **52**, 3489 (1995).

[23] Y. Soudagar, F. Bussières, G. Berlin, S. Lacroix, J. M. Fernandez, and N. Godbout, JOSA B (to be published) (2006).

[24] A. Garg and N. D. Mermin, Phys. Rev. D **35**, 3831 (1987).

[25] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, Phys. Rev. A **71**, 061803(R) (2005).

[26] D. Stucki, H. Zbinden, and N. Gisin, J. of Mod. Optics **52**, 2637 (2005).

[27] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).

[28] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).